UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/577,111	04/25/2006	Hideki Imai	P/2850-136	4333

2352 7590 07/21/2009
OSTROLENK FABER GERB & SOFFEN
1180 AVENUE OF THE AMERICAS
NEW YORK, NY 100368403

EXAMINER	
CHEN, SHIN HON	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
07/21/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/577,111	IMAI ET AL.	
	Examiner	Art Unit	
	SHIN-HON CHEN	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 April 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-50* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *1-8,22-30 and 44-48* is/are allowed.

6)☒ Claim(s) *31-43* is/are rejected.

7)☒ Claim(s) *9-19,31-43,49 and 50* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 April 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *4/25/06*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-50 have been examined.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 4/25/06 is being considered by the examiner.

Claim Objections

3. Claims 9-19, 31-43, 49 and 50 are objected to because of the following informalities: The identified claim disclose an authentication program that is used by server and client devices, however, the program itself could be embodied in carrier wave or signals. Therefore, applicant is advised to amend the claims to disclose a computer readable storage medium storing authentication program to avoid potential 101 rejection. Appropriate correction is required.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 31-43 are rejected under 35 U.S.C. 102(e) as being anticipated by Peyravian et al. U.S. Pub. No. 20040158708 (hereinafter Peyravian).

6. As per claim 31, Peyravian discloses an authentication program that runs on a terminal of an authentication system for mutual authentication between a terminal and a server wherein the program allows a computer to execute: a memory process to pre-store an authentication information P' for terminal storage and an RSA public key (N, e) (Peyravian: figure 1: ID and public key); a concatenation process to yield a value W using a specific calculation formula with the input of the stored authentication information P' and a password entered for authentication (Peyravian: figure 1 step 115: password and ID); and a mask operation process to yield a value Z using a specific calculation formula with the input of the value W, the stored RSA public key (N, e), and an internally generated random number T, and then send Z to the server (Peyravian: figure 1: step 115: generating ARGc based on ID, password, public key, and random number; [0010]).

7. As per claim 32, Peyravian discloses the authentication program according to claim 31. Peyravian further discloses wherein the program further allows a computer to execute a data extension process to yield authentication information P1 based on a password previously-determined by the user (Peyravian: [0010]: secret password known by both client and server).

8. As per claim 33, Peyravian discloses the authentication program according to claim 31. Peyravian further discloses wherein the program further allows a computer to execute an RSA key generation process to yield the RSA public key (N, e) (Peyravian: figure 1: step 110).

9. As per claim 34, Peyravian discloses the authentication program according to claim 31. Peyravian further discloses wherein the program further allows a computer to execute: an authentication result verification process to compare a value V2 received from the server with a value V2 obtained using a specific calculation formula with the input of the random number T and, if they match, authenticate the server; and a verifier generation process to yield a value V1 using a specific calculation formula with the input of the random number T and send V1 to the server (Peyravian: figure 3: step 340).

10. As per claim 35, Peyravian discloses an authentication program that runs on a server of an authentication system for mutual authentication between a terminal and a server wherein the program allows a computer to execute: a memory process to pre-store a password verification data H for server registration and an RSA private key (N, d) (Peyravian: figure 1: 140); and a master key generation process to yield a value T using a specific calculation formula with the input of the stored password verification data H, RSA private key (N, d) and a value Z received from the terminal (Peyravian: figure 1: 140).

11. As per claim 36, Peyravian discloses the authentication program according to claim 35. Peyravian further discloses wherein the program further allows a computer to execute a data extension process to yield the password verification data H based on a password previously-determined by the user (Peyravian: [0010]: password known by both client and server).

12. As per claim 37, Peyravian discloses the authentication program according to claim 35. Peyravian further discloses wherein the program further allows a computer to execute an RSA key generation process to yield the RSA private key (N, d) (Peyravian: [0010]).

13. As per claim 38, Peyravian discloses the authentication program according to claim 35. Peyravian further discloses wherein the program further allows a computer to execute: a verifier generation process to yield a value V2 using a specific calculation formula with the input of the value T and send V2 to the terminal; and an authentication result verification process to compare a value V1 received from the server with a value V1 obtained using a specific calculation formula with the input of the value T and, if they match, to authenticate the terminal (Peyravian: figure 3: step 340).

14. As per claim 39, Peyravian discloses the authentication program according to claim 34. Peyravian further discloses wherein each of the terminal and the server comprises a session key generation process to generate a session key when they are mutually authenticated (Peyravian: figure 4).

15. As per claim 40, Peyravian discloses the authentication program according to claim 31. Peyravian further discloses wherein that the authentication information P' is a polynomial equation and an FDH function (Peyravian: [0010]).

16. As per claim 41, Peyravian discloses the authentication program according to claim 31. Peyravian further discloses wherein the authentication information P1 is an FDH function (Peyravian: [0010]).

17. As per claim 42, Peyravian discloses the authentication program according to claim 31. Peyravian further discloses wherein the RSA public key (N, e) uses secure communication (Peyravian: [0010]: the communication can be either secure or insecure because the content itself is encrypted and hashed to ensure security).

18. As per claim 43, Peyravian discloses the authentication program according to claim 31. Pyeravian further discloses wherein the RSA public key (N, e) uses insecure communication (Peyravian: [0010]: the communication can be either secure or insecure because the content itself is encrypted and hashed to ensure security).

Conclusion

19. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Eldridge et al. U.S. Pat. No. 6061799 discloses removable media for password based authentication in a distributed system.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SHIN-HON CHEN whose telephone number is (571)272-3789. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William R. Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Shin-Hon Chen
Primary Examiner
Art Unit 2431

/Shin-Hon Chen/
Primary Examiner, Art Unit 2431